ACTA ARITHMETICA
XLIV (1984)

A construction of unramified Abelian l-extensions of regular Kummer extensions

by

NORIKATA NAKAGOSHI (Toyama, Japan)

1. Introduction. For the quadratic fields the genus theory of Gauss shows that the genus fields are determined by the 2nd roots of "prime discriminant". Here we deal with a Kummer extension generated by the lth root of a positive rational integer m over the regular lth cyclotomic field k. We shall construct the l-genus field (cf. § 2) of $k(\sqrt[l]{m})$ over k as a Kummer extension which is generated by the adjunctions of the lth roots of rational integers and "Primärzahlen" [6] of prime ideals of k to k. For each prime factor p of m satisfying the congruence $p^{l-1} \equiv 1 \bmod l^2$ we assume that the order of p modulo l is even when $l \geqslant 5$.

For an algebraic number field F of finite degree over the field Q of rationals, we denote by h_F and E_F the class number of F and the group of units of F respectively.

Let l be a prime number. If L/F is an Abelian extension whose Galois group is of type $(l, \ldots, l)$, then we say that the extension L/F is of type $(l, \ldots, l)$. We shall use the notation $\alpha \underset{(l)}{=} \beta$ in F if α/β is the lth power of a number of F. If l is odd and d is a real number, then we let $\sqrt[l]{d}$ be the real lth root of d.

We denote by $g_{L/F}$ the genus number of a Galois extension L over F. It is determined by Y. Furuta [3]. If L/F is a cyclic extension, then $g_{L/F}$ is equal to the number $a_{L/F}$ of ambiguous ideal classes with respect to L over F.

2. Regular Kummer extensions $k(\sqrt[l]{p})$ and the l-genus fields. Let $l \geqslant 3$ be a regular prime and ζ be a primitive lth root of unity. We set $k = Q(\zeta)$. We call an extension $k(\sqrt[l]{\mu})$ for $\mu \in k$ a *regular Kummer extension* generated by μ.

Let $F = k(\sqrt[l]{\mu})$. We denote by $F^*(l)$ or $k^*(l, \mu)$ the l-genus field of F over k, that is, $F^*(l) = k^*(l, \mu)$ is a subfield of the genus field of F over k and the degree $(F^*(l): F)$ is equal to the l-component of $g_{F/k}$. Since l is regular, $F^*(l)/k$ is an extension of type $(l, \ldots, l)$ (cf. [7], Proposition 2). In this section we shall construct $k^*(l, p)$ as a Kummer extension of k for a rational prime $p \neq l$.

Now the class number h_k of the regular lth cyclotomic field k is prime to l. There exists a rational integer $h^* > 0$ such that $h_k h^* \equiv 1 \bmod l$. Let $\mathfrak{l} = (1-\zeta)$ be the prime ideal of k dividing l and $k_0 = Q(\zeta+\zeta^{-1})$ be the maximal real subfield of k. We denote by $\bar{\alpha}$ the complex conjugate of a number α of k.

Let $\mathfrak{p}$ be a prime ideal of k, prime to $\mathfrak{l}$. We can set

$$\mathfrak{p}^{h_k h^*} = (\pi)$$

where π is a "Primärzahl von $\mathfrak{p}$" (cf. [6], Satz 157 in § 142); π is congruent to a rational integer modulo $\mathfrak{l}^2$ and $\pi\bar{\pi}$ is congruent to a rational integer modulo $\mathfrak{l}^{l-1}$.

LEMMA 1. *Let $l \geqslant 3$ be a regular prime.*

(i) *If π and π' are "Primärzahlen von $\mathfrak{p}$", then π/π' is the l-th power of a unit of E_{k_0}.*

(ii) *The class number of $k(\sqrt[l]{\pi})$ is prime to l.*

Proof. (i) There exists a unit ε of k such that $\pi' = \varepsilon\pi$. Since $\pi\bar{\pi}$ and $\pi'\bar{\pi}'$ are congruent to rational integers modulo $\mathfrak{l}^{l-1}$, respectively, $\varepsilon\bar{\varepsilon}$ is also congruent to a rational integer modulo $\mathfrak{l}^{l-1}$. By Hilbert's Theorem 156 (cf. [1], Chap. V, § 6, Satz 3) we see that $\varepsilon\bar{\varepsilon}$ is the lth power of a unit of E_k. Kummer's Lemma ([1], Chap. III, § 1, Lemma 4) shows that $\varepsilon = \zeta^a \varepsilon_{01}$ with $0 \leqslant a \leqslant l-1$ and $\varepsilon_{01} \in E_{k_0}$. Hence $\varepsilon\bar{\varepsilon} = \varepsilon_{01}^2$ and also $\varepsilon_{01} \in E_{k_0}^l$. We set $\varepsilon = \zeta^a \varepsilon_{02}^l$ with $\varepsilon_{02} \in E_{k_0}$.

Moreover, π and π' are congruent to rational integers modulo $\mathfrak{l}^2$, respectively. Hence $\varepsilon = \zeta^a \varepsilon_{02}^l \equiv \Delta \bmod \mathfrak{l}^2$ for some rational integer Δ. We have $\zeta^{a(l-1)} \varepsilon_{02}^{l(l-1)} \equiv \Delta^{l-1} \bmod \mathfrak{l}^2$ and $\zeta^{a(l-1)} \equiv 1 \bmod \mathfrak{l}^2$. Therefore $a \equiv 0 \bmod l$, as desired.

(ii) Let $k' = k(\sqrt[l]{\pi})$. It follows from [5] that

$$a_{k'/k} = h_k l^\delta / (E_k : E_k \cap N_{k'/k} k')$$

where $N_{k'/k}$ is the norm map from k' to k and $\delta = 1$ or 0 according as $\mathfrak{l}$ is ramified in k', or not.

If $\mathfrak{p}$ is the "Primideal erster Art" ([6], Hilfssatz 37 in § 155), then $(E_k : E_k \cap N_{k'/k} k') \neq 1$ and $\mathfrak{l}$ is ramified in k'. Hence $a_{k'/k} = h_k$ which is prime to l.

If $\mathfrak{p}$ is the "Primideal zweiter Art" ([6], Hilfssatz 37 and Hilfssatz 43), then $\mathfrak{l}$ is unramified in k'. Hence $a_{k'/k} = h_k$.

It is shown in [13] that $h_{k'} \equiv a_{k'/k} \bmod l$. Thus we have (ii).

It is clear that the regular Kummer extension generated by a "Primärzahl von $\mathfrak{p}$" over k is uniquely determined by $\mathfrak{p}$.

Let

$$p = \mathfrak{p}_1 \ldots \mathfrak{p}_g$$

be the decomposition of p into prime ideals of k. For each $i = 1, \ldots, g$ we can set

$$\mathfrak{p}_i^{h_k h^*} = (\pi_i)$$

where π_i is a "Primärzahl von $\mathfrak{p}_i$".

LEMMA 2. *Let $l \geqslant 3$ be a regular prime. Then $p^{h_k h^*}$ is written in the form*

$$p^{h_k h^*} = \varepsilon_0^l \pi_1 \ldots \pi_g \tag{1}$$

for some unit ε_0 of E_{k_0}.

Proof. There is a unit ε_1 of k such that $p^{h_k h^*} = \varepsilon_1 \pi_1 \ldots \pi_g$. Since $\pi_i\bar{\pi}_i$ is congruent to a rational integer modulo $\mathfrak{l}^{l-1}$ for each $i = 1, \ldots, g$, $p^{2h_k h^*} \equiv \varepsilon_1 \bar{\varepsilon}_1 \Delta_1 \bmod \mathfrak{l}^{l-1}$ for some rational integer Δ_1. Then $\varepsilon_1 \bar{\varepsilon}_1$ is congruent to a rational integer modulo $\mathfrak{l}^{l-1}$. By the proof of (i) of Lemma 1 we see that $\varepsilon_1 = \zeta^b \varepsilon_0^l$ with $0 \leqslant b \leqslant l-1$ and $\varepsilon_0 \in E_{k_0}$.

Moreover, π_i is congruent to a rational integer modulo $\mathfrak{l}^2$ for each $i = 1, \ldots, g$. Hence $p^{h_k h^*} \equiv \zeta^b \varepsilon_0^l \Delta_2 \bmod \mathfrak{l}^2$ for some rational integer Δ_2. Then we have $p^{h_k h^*(l-1)} \equiv \zeta^{b(l-1)} \varepsilon_0^{l(l-1)} \Delta_2^{l-1} \bmod \mathfrak{l}^2$ and also $\zeta^{b(l-1)} \equiv 1 \bmod \mathfrak{l}^2$. Thus $b \equiv 0 \bmod l$.

Lemma 2 ensures that $k(\sqrt[l]{p})$ is a subfield of $k(\sqrt[l]{\pi_1}, \ldots, \sqrt[l]{\pi_g})$.

LEMMA 3. *Let $l \geqslant 3$ be a regular prime and ε be a unit of k such that $\varepsilon \underset{(l)}{\neq} 1$ in k. Then $\mathfrak{l}$ is ramified in $k(\sqrt[l]{\varepsilon \pi_1^{r_1} \ldots \pi_g^{r_g}})$ where $r_1, \ldots, r_g$ are arbitrary rational integers.*

Proof. Since l is regular, $k(\sqrt[l]{\varepsilon})$ is a ramified extension of k for each unit ε with $\varepsilon \underset{(l)}{\neq} 1$ in k which is unramified outside $\mathfrak{l}$.

We assume that $\mathfrak{l}$ is unramified in $k(\sqrt[l]{\varepsilon \pi_1^{r_1} \ldots \pi_g^{r_g}})$ for a unit ε with $\varepsilon \underset{(l)}{\neq} 1$ in k. It then follows from [5, Teil $\mathrm{I_a}$, § 11], that there exists an integer x of k such that

$$x^l \equiv \varepsilon \pi_1^{r_1} \ldots \pi_g^{r_g} \bmod \mathfrak{l}^l.$$

Since $\mathfrak{l}$ is an ambiguous ideal of k over Q, we have

$$\bar{x}^l \equiv \bar{\varepsilon} \bar{\pi}_1^{r_1} \ldots \bar{\pi}_g^{r_g} \bmod \mathfrak{l}^l.$$

Hence

$$(x\bar{x})^{l(l-1)} \equiv (\varepsilon\bar{\varepsilon})^{l-1} \{(\pi_1\bar{\pi}_1)^{r_1} \ldots (\pi_g\bar{\pi}_g)^{r_g}\}^{l-1} \bmod \mathfrak{l}^l,$$

where $\pi_i\bar{\pi}_i$ is congruent to a rational integer modulo $\mathfrak{l}^{l-1}$ for each $i = 1, \ldots, g$ and also $(\pi_i\bar{\pi}_i)^{l-1} \equiv 1 \bmod \mathfrak{l}^{l-1}$. It follows from [9] that the group of prime residue classes modulo $\mathfrak{l}^{l-1}$ in k is of type $(l-1, l, \ldots, l)$. Hence $(\varepsilon\bar{\varepsilon})^{l-1} \equiv 1 \bmod \mathfrak{l}^{l-1}$. Then $\varepsilon\bar{\varepsilon} = (\varepsilon\bar{\varepsilon})^l/(\varepsilon\bar{\varepsilon})^{l-1}$ and by the same proof of (i) of Lemma 1 we obtain $\varepsilon = \zeta^c \varepsilon_0'^l$ with $0 \leqslant c \leqslant l-1$ and $\varepsilon_0' \in E_{k_0}$.

Moreover, π_i is congruent to a rational integer modulo $\mathfrak{l}^2$ for each

$i = 1, \ldots, g$. Hence $x^l \equiv \zeta^c \varepsilon_0'^l \Delta_3 \bmod \mathfrak{l}^2$ for some rational integer Δ_3. Then we have $x^{l(l-1)} \equiv \zeta^{c(l-1)} \varepsilon_0'^{l(l-1)} \Delta_3^{l-1} \bmod \mathfrak{l}^2$ and also $\zeta^{c(l-1)} \equiv 1 \bmod \mathfrak{l}^2$. Thus $c \equiv 0 \bmod l$ which implies $\varepsilon \underset{(l)}{=} 1$ in k, contradiction.

If $l = 2$, then Lemma 3 is not true. For example, 2 is unramified in $Q(\sqrt{-p})$ where p is a prime number such that $p \equiv -1 \bmod 4$; 2 and the infinite prime divisor of Q are ramified in $Q(\sqrt{-1})$.

Lemma 4. *Let L/F be an extension of type (l, l) and $F_0, F_1, \ldots, F_l$ be cyclic subfields of L, of degree l over F.*

Then there exists a prime ideal $\mathfrak{q}$ of F which is totally ramified in L if and only if $\mathfrak{q}$ is ramified in all $F_0, F_1, \ldots, F_l$.

Proof. The inertia field of $\mathfrak{q}$ with respect to L/F is F.

Proposition 1. *Let $l \geq 3$ be a regular prime. Then $k^*(l, p)$ is a subfield of $k(\sqrt[l]{\pi_1}, \ldots, \sqrt[l]{\pi_g})$.*

Proof. Let $F = k(\sqrt[l]{p})$. If F' is a cyclic extension of degree l over k and FF' is an unramified extension of F, then prime divisors of k which are ramified in F' are at most $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ and $\mathfrak{l}$. Hence we can set $F' = k\left(\sqrt[l]{\varepsilon(1-\zeta)^r \pi_1^{r_1} \ldots \pi_g^{r_g}}\right)$ where ε is a unit of k and $r, r_1, \ldots, r_g$ are rational integers.

Since $k^*(l, p)/k$ is of type $(l, \ldots, l)$, it will suffice to show that if $\varepsilon \underset{(l)}{\neq} 1$ in k or $r \not\equiv 0 \bmod l$, then FF' is a ramified extension of F.

If $r \not\equiv 0 \bmod l$ and $\mathfrak{l}$ is unramified in F, then FF' is a ramified extension of F. If $r \not\equiv 0 \bmod l$ and $\mathfrak{l}$ is ramified in F, then $\mathfrak{l}$ is ramified in all intermediate fields F, $k\left(\sqrt[l]{p^s \varepsilon (1-\zeta)^r \pi_1^{r_1} \ldots \pi_g^{r_g}}\right)$ of FF' over k ($s = 0, 1, \ldots, l-1$). Hence $\mathfrak{l}$ is totally ramified in FF' by Lemma 4. Therefore, if $r \not\equiv 0 \bmod l$, then FF' is a ramified extension of F.

Now we assume that $\varepsilon \underset{(l)}{\neq} 1$ in k and $r = 0$. Then we see by Lemma 2 that $F \neq F'$. If $\mathfrak{l}$ is unramified in F, then FF' is a ramified extension of F, since $\mathfrak{l}$ is ramified in F' by Lemma 3.

If $\mathfrak{l}$ is ramified in F and FF' is an unramified extension of F, then $\mathfrak{l}$ is not totally ramified in FF'. By Lemma 4 there exists a rational integer s $(1 \leq s \leq l-1)$ such that $\mathfrak{l}$ is unramified in $k\left(\sqrt[l]{p^s \varepsilon \pi_1^{r_1} \ldots \pi_g^{r_g}}\right)$. By Lemma 2 it is contrary to Lemma 3. Hence, if $\varepsilon \underset{(l)}{\neq} 1$ in k, then FF' is a ramified extension of F.

Thus we see that $F' = k(\sqrt[l]{\pi_1^{r_1} \ldots \pi_g^{r_g}})$ for some rational integers $r_1, \ldots, r_g$ which is a subfield of $k(\sqrt[l]{\pi_1}, \ldots, \sqrt[l]{\pi_g})$.

We note from [11] that $\mathfrak{l}$ is unramified in a Kummer extension $k(\sqrt[l]{m})$ if and only if $m^{l-1} \equiv 1 \bmod l^2$ where m is a positive lth power free rational integer.

Proposition 2. *Let $F = k(\sqrt[l]{p})$ be a regular Kummer extension generated by a rational prime p such that $p^{l-1} \not\equiv 1 \bmod l^2$ and $p \neq l$.*

Then we have

$$(E_k : E_k \cap N_{F/k}F) = l.$$

Proof. We consider regular Kummer extensions $k_i = k(\sqrt[l]{\pi_i})$ and the Hilbert norm residue symbols $\left(\frac{\varepsilon, p}{\mathfrak{p}_i}\right)$ for $i = 1, \ldots, g$ and $\varepsilon \in E_k$. We have by (1)

$$\left(\frac{\varepsilon, p}{\mathfrak{p}_i}\right)^{h_k h^*} = \left(\frac{\varepsilon, p^{h_k h^*}}{\mathfrak{p}_i}\right) = \left(\frac{\varepsilon, \pi_i}{\mathfrak{p}_i}\right), \tag{2}$$

since $\mathfrak{p}_i$ is unramified in $k(\sqrt[l]{\varepsilon})$ and k_j for $j \neq i$. On the other hand

$$\left(\frac{\varepsilon, p}{\mathfrak{p}_i}\right) = \left(\frac{p, \varepsilon}{\mathfrak{p}_i}\right)^{-1} = \left(\frac{\varepsilon}{\mathfrak{p}_i}\right)$$

where $\left(\frac{\varepsilon}{\mathfrak{p}_i}\right)$ is the lth power residue symbol defined by $\left(\frac{\varepsilon}{\mathfrak{p}_i}\right)\sqrt[l]{\varepsilon} = \left(\frac{k(\sqrt[l]{\varepsilon})}{\mathfrak{p}_i}\right)\sqrt[l]{\varepsilon}$ and $\left(\frac{k(\sqrt[l]{\varepsilon})}{\mathfrak{p}_i}\right)$ is the Artin symbol of $k(\sqrt[l]{\varepsilon})$ over k. Let f be the order of p modulo l. It then follows that

$$\left(\frac{\zeta, p}{\mathfrak{p}_i}\right) = 1 \Leftrightarrow \left(\frac{\zeta}{\mathfrak{p}_i}\right) = 1$$

$\Leftrightarrow \mathfrak{p}_i$ splits completely in the l^2-th cyclotomic field $k(\sqrt[l]{\zeta})$ $\Leftrightarrow p^f \equiv 1 \bmod l^2 \Leftrightarrow p^{l-1} \equiv 1 \bmod l^2$.

Hence, if $p^{l-1} \not\equiv 1 \bmod l^2$, then ζ is not a norm in k_i/k, that is, $(E_k : E_k \cap N_{k_i/k} k_i) \geq l$ for $i = 1, \ldots, g$.

The number $a_{k_i/k}$ of ambiguous ideal classes of k_i over k is given by $a_{k_i/k} = h_k l^\delta / (E_k : E_k \cap N_{k_i/k} k_i)$, where $\delta = 1$ or 0 according as $\mathfrak{l}$ is ramified in k_i, or not. Since $h_{k_i} \equiv a_{k_i/k} \bmod l$ and h_{k_i} is prime to l for each i by Lemma 1, $\mathfrak{l}$ is ramified in all $k_1, \ldots, k_g$. Therefore we have $(E_k : E_k \cap N_{k_i/k} k_i) = l$ for $i = 1, \ldots, g$. Thus it follows from (2) that $(E_k : E_k \cap N_{F/k} F) = l$.

Proposition 3. *Let $F = k(\sqrt[l]{p})$ be a regular Kummer extension generated by a rational prime p such that $p^{l-1} \equiv 1 \bmod l^2$. Let f be the order of p modulo l. If f is even, or $l = 3$, then*

$$(E_k : E_k \cap N_{F/k}F) = 1.$$

Proof. Let N be a number of odd n with $1 < n < l$ such that $p^n \not\equiv 1 \bmod l$. If f is even, then $N = (l-1)/2 - 1$. It follows from Theorem 5 of [10] that $(E_k \cap N_{F/k} F : E_k^l) \geq l^{N+1}$ and also $(E_k : E_k \cap N_{F/k} F) = 1$.

If $l=3$, then ζ is a norm in F/k, because $p^{l-1}\equiv 1 \bmod l^2$.

Assume that $l\equiv 3 \bmod 4$, $p^{l-1}\equiv 1 \bmod l^2$ and $f=(l-1)/2\neq 1$. If $p^{h'}=(x^2+ly^2)/4$ for some rational integers x, y with $y\not\equiv 0 \bmod l$ where h' is the class number of $Q(\sqrt{-l})$, then we see by Theorem 8 of [10] that the class number of $F=k(\sqrt[l]{p})$ is prime to l. In this case $\mathfrak{l}$ is unramified in F and $a_{F/k}=h_k l/(E_k:E_k\cap N_{F/k}F)$. Thus we have $(E_k:E_k\cap N_{F/k}F)=l$, since $h_F\equiv a_{F/k} \bmod l$.

THEOREM 1. *Let $k(\sqrt[l]{p})$ be a regular Kummer extension generated by a rational prime $p\neq l$. If $p^{l-1}\equiv 1 \bmod l^2$ and E_k is contained in $N_{k(\sqrt[l]{p})/k}(k(\sqrt[l]{p}))$, or if $p^{l-1}\not\equiv 1 \bmod l^2$, then*

$$k^*(l,p)=k(\sqrt[l]{\pi_1},\ldots,\sqrt[l]{\pi_g})$$

is the l-genus field of $k(\sqrt[l]{p})$ over k and $(k^*(l,p):k(\sqrt[l]{p}))=l^{g-1}$.

Proof. If $p^{l-1}\equiv 1 \bmod l^2$ and $E_k\subset N_{k(\sqrt[l]{p})/k}(k(\sqrt[l]{p}))$, then $\mathfrak{l}$ is unramified in $k(\sqrt[l]{p})$ and $g_{k(\sqrt[l]{p})/k}=a_{k(\sqrt[l]{p})/k}=h_k l^{g-1}$. If $p^{l-1}\not\equiv 1 \bmod l^2$, then $\mathfrak{l}$ is ramified in $k(\sqrt[l]{p})$ and $g_{k(\sqrt[l]{p})/k}=a_{k(\sqrt[l]{p})/k}=h_k l^{g-1}$ by Proposition 2. Since $k(\sqrt[l]{p})$ is a subfield of $k(\sqrt[l]{\pi_1},\ldots,\sqrt[l]{\pi_g})$ by Proposition 1, we have

$$k^*(l,p)=k(\sqrt[l]{\pi_1},\ldots,\sqrt[l]{\pi_g}).$$

3. Regular Kummer extensions $k(\sqrt[l]{m})$ and the l-genus fields. If $l=3$, the constructions of the genus fields of $k(\sqrt[3]{m})$ are explicitly given by H. Wada [12] and F. Gerth III [4]. In this section we let $l\geqslant 5$ be a regular prime and $k=Q(\zeta)$ be the lth cyclotomic field.

In order to construct an unramified extension of a number field we need the following three lemmas.

ABHYANKER'S LEMMA (cf. [2] and [8]). *Let $L=L_1L_2$ be a composite of number fields L_1 and L_2 of finite degree over a number field F. Let $\mathfrak{P}$ be a prime ideal of L lying over a prime ideal $\mathfrak{p}_i$ of L_i for each $i=1,2$. Let e_i be the ramification index of $\mathfrak{p}_i$ over F for each $i=1,2$.*

If $\mathfrak{p}_2$ is tamely ramified over F and $e_1\equiv 0 \bmod e_2$, then L/L_1 is an unramified extension at $\mathfrak{P}$.

Let p be a prime number such that $p\neq l$ and $p^{l-1}\not\equiv 1 \bmod l^2$. Then $\mathfrak{l}$ is ramified in all $k(\sqrt[l]{\pi_1}),\ldots,k(\sqrt[l]{\pi_g})$ by Proposition 2.

LEMMA 5. *Let p be a prime number such that $p\neq l$, $p^{l-1}\not\equiv 1 \bmod l^2$ and $g\geqslant 2$. Then there exist rational integers a_i $(1\leqslant a_i\leqslant l-1)$ such that $\mathfrak{l}$ is unramified in $k(\sqrt[l]{\pi_1^{a_i}\pi_i})$ for $i=2,\ldots,g$.*

Proof. If $\mathfrak{l}$ is ramified in $k(\sqrt[l]{\pi_1\pi_i})$, $k(\sqrt[l]{\pi_1^2\pi_i}),\ldots,k(\sqrt[l]{\pi_1^{l-1}\pi_i})$ for $i\neq 1$, then $\mathfrak{l}$ is totally ramified in $k(\sqrt[l]{\pi_1},\sqrt[l]{\pi_i})$ which is contrary to the fact $k^*(l,p)=k(\sqrt[l]{\pi_1},\ldots,\sqrt[l]{\pi_g})$ is the l-genus field of $k(\sqrt[l]{p})$ over k by Theorem 1.

LEMMA 6. *Let d_1 and d_2 be the l-th power free rational integers, prime to l. Let $d_1 \underset{(l)}{\neq} d_2$ in k. Then $\mathfrak{l}$ is not totally ramified in $k(\sqrt[l]{d_1},\sqrt[l]{d_2})$.*

Proof. If $d_1^{l-1}\equiv 1$ or $d_2^{l-1}\equiv 1 \bmod l^2$, then $\mathfrak{l}$ is unramified in $k(\sqrt[l]{d_1})$ or $k(\sqrt[l]{d_2})$.

If $d_1^{l-1}=1+lx_1$ and $d_2^{l-1}=1+lx_2$ for some rational integers x_1, x_2, prime to l, then there exists a rational integer r $(1\leqslant r\leqslant l-1)$ such that $rx_1+x_2\equiv 0 \bmod l$. Hence

$$(d_1^r d_2)^{l-1}=(1+lx_1)^r(1+lx_2)\equiv 1 \bmod l^2.$$

Therefore $\mathfrak{l}$ is unramified in $k(\sqrt[l]{d_1^r d_2})$ which is a subfield of $k(\sqrt[l]{d_1},\sqrt[l]{d_2})$.

Let m be a positive lth power free rational integer, prime to l. For each prime factor of p of m, let f_p be the order of p modulo l and $g_p=(l-1)/f_p$ be the number of distinct prime factors of p in the lth cyclotomic field k.

First we construct the l-genus field of $k(\sqrt[l]{m})$ over k where every prime factor p of m satisfies $p^{l-1}\equiv 1 \bmod l^2$ and f_p is even. Let $k^*(l,p)$ be the l-genus field of $k(\sqrt[l]{p})$ over k given by Theorem 1. We note that $k(\sqrt[l]{m})$ is a subfield of $\prod_{p|m} k^*(l,p)$. Then we prove the following

THEOREM 2. *Let $l\geqslant 5$ be a regular prime and m be a positive l-th power free rational integer, prime to l. Let $K^*(l)$ be the l-genus field of $K=k(\sqrt[l]{m})$ or $K=k(\sqrt[l]{lm})$ over k. If $p^{l-1}\equiv 1 \bmod l^2$ and f_p is even for each prime factor p of m, then*

$$K^*(l)=K\prod_{p|m} k^*(l,p),$$

$$(K^*(l):K)=\begin{cases}\prod_{p|m} l^{g_p}/l, & \text{if } K=k(\sqrt[l]{m}),\\ \prod_{p|m} l^{g_p}, & \text{if } K=k(\sqrt[l]{lm});\end{cases}$$

and $(E_k:E_k\cap N_{K/k}K)=1$.

Proof. (i) Let $K=k(\sqrt[l]{m})$. Then $\mathfrak{l}$ is unramified in K and $k^*(l,p)$ for all $p|m$. Applying Proposition 3 and Theorem 1 we have $(\prod_{p|m} k^*(l,p):K)=\prod_{p|m} l^{g_p}/l$, since K is a subfield of $\prod_{p|m} k^*(l,p)$. It follows from Abhyanker's Lemma that $K\cdot\prod_{p|m} k^*(l,p)=\prod_{p|m} k^*(l,p)$ is an unramified Abelian extension of K and also a subfield of $K^*(l)$. Hence $(K^*(l):K)\geqslant\prod_{p|m} l^{g_p}/l$. By the genus number formula [3] of K over k we obtain

$$(K^*(l):K) = \prod_{p|m} l^{g_p}/l(E_k : E_k \cap N_{K/k}K)$$

which is equal to the l-component of $a_{K/k} = g_{K/k}$. Thus

$$(E_k : E_k \cap N_{K/k}K) = 1 \quad \text{and} \quad K^*(l) = \prod_{p|m} k^*(l, p).$$

(ii) Let $K = k(\sqrt[l]{lm})$. Then $\mathfrak{l}$ is ramified in K but unramified in $k^*(l, p)$ for all $p|m$ which shows that $K \cap \prod_{p|m} k^*(l, p) = k$. Applying Abhyanker's Lemma and Theorem 1 we see that $K \cdot \prod_{p|m} k^*(l, p)$ is an unramified Abelian extension of degree $\prod_{p|m} l^{g_p}$ over K and a subfield of $K^*(l)$. Hence $(K^*(l):K) \geqslant \prod_{p|m} l^{g_p}$. By the genus number formula of K over k we obtain

$$(K^*(l):K) = l\prod_{p|m} l^{g_p}/l(E_k : E_k \cap N_{K/k}K) = \prod_{p|m} l^{g_p}/(E_k : E_k \cap N_{K/k}K).$$

Thus

$$(E_k : E_k \cap N_{K/k}K) = 1 \quad \text{and} \quad K^*(l) = K \cdot \prod_{p|m} k^*(l, p).$$

Secondly we shall construct the l-genus field of $k(\sqrt[l]{m})$ over k where m is divisible by primes p such that $p^{l-1} \not\equiv 1 \bmod l^2$.

Let m be a positive lth power free rational integer satisfying the following conditions:

(3) $$(m, l) = 1;$$

(4) $m = m_0 m_1$ where $q^{l-1} \equiv 1 \bmod l^2$ and f_q is even for each prime factor q of m_0, $m_1 = p_1 \ldots p_t$ and $p_j^{l-1} \not\equiv 1 \bmod l^2$ for $j = 1, \ldots, t$ $(t \geqslant 1)$.

For each prime factor p of m_1 we obtain the l-genus field $k^*(l, p) = k(\sqrt[l]{\pi_1}, \ldots, \sqrt[l]{\pi_{g_p}})$ of $k(\sqrt[l]{p})$ over k. We note that $\mathfrak{l}$ is ramified in $k(\sqrt[l]{p})$. By Lemma 5, let a_i $(1 \leqslant a_i \leqslant l-1)$ be rational integers such that $\mathfrak{l}$ is unramified in $k(\sqrt[l]{\pi_1^{a_i}\pi_i})$ for $i = 2, \ldots, g_p$, if $g_p \geqslant 2$. We define

(5) $$k_1'(l, m_1) = \prod_{\substack{p|m_1\\ g_p>1}} k(\sqrt[l]{\pi_1^{a_2}\pi_2}, \ldots, \sqrt[l]{\pi_1^{a_{g_p}}\pi_{g_p}}).$$

Then

$$(k_1'(l, m_1):k) = \prod_{p|m_1} l^{g_p-1},$$

because $\prod_{\substack{p|m_1\\ g_p>1}} (\pi_1^{a_2}\pi_2)^{c_2} \ldots (\pi_1^{a_{g_p}}\pi_{g_p})^{c_{g_p}} \underset{(l)}{=} 1$ in k if and only if $c_2 \equiv \ldots \equiv c_{g_p} \equiv 0 \bmod l$ for all $p|m_1$ with $g_p > 1$. If $g_p = 1$ for all prime factors p of m_1, we set $k_1'(l, m_1) = k$.

Lemma 6 ensures that there exist rational integers b_j such that $\mathfrak{l}$ is unramified in $k(\sqrt[l]{p_1^{b_j}p_j})$ for $j = 2, \ldots, t$, if $t \geqslant 2$. We define

(6) $$k_2'(l, m_1) = \begin{cases} k, & \text{if} \quad t = 1, \\ \prod_{j=2}^{t} k(\sqrt[l]{p_i^{b_j}p_j}), & \text{if} \quad t \geqslant 2. \end{cases}$$

Then $(k_2'(l, m_1):k) = l^{t-1}$.

Let $K_0 = k(\sqrt[l]{m_0})$. Then

(7) $$K_0^*(l) = \prod_{q|m_0} k^*(l, q)$$

is the l-genus field of K_0 over k which is given by Theorem 2. We should note that $(K_0^*(l):k) = \prod_{q|m_0} l^{g_q}$.

We now obtain the following result:

Lemma 7. *Let m be the l-th power free rational integer satisfying* (3) *and* (4). *Then we have*:

(i) $(k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l):k) = \prod_{p|m} l^{g_p}/l$.

(ii) *If* $m^{l-1} \equiv 1 \bmod l^2$ *and* $K = k(\sqrt[l]{m})$, *then* K *is a subfield of* $k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l)$.

Proof. (i) If $t = 1$, then $m_1 = p_1$ and $k_2'(l, m_1) = k$. Since l is regular, $k_1'(l, m_1) \cap K_0^*(l) = k$. Hence we have

$$(k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l):k) = l^{g_{p_1}-1} \cdot 1 \cdot \prod_{q|m_0} l^{g_q} = \prod_{p|m} l^{g_p}/l.$$

Let $t \geqslant 2$. Since l is regular, $k_1'(l, m_1) \cdot k_2'(l, m_1) \cap K_0^*(l) = k$. We see that the first assertion will be proved if we show that $k_1'(l, m_1) \cap k_2'(l, m_1) = k$. If $g_p = 1$ for all prime factors p of m_1, then $k_1'(l, m_1) = k$. Assume that $g_{p_1} > 1$. If $k(\sqrt[l]{\mu})$ is a subfield of $k_1'(l, m_1) \cap k_2'(l, m_1)$, then by Kummer theory μ is written in the form

(8) $$\mu \underset{(l)}{=} \prod_{\substack{p|m_1\\ g_p>1}} \pi_1^{\Sigma a_i x_i} \pi_2^{x_2} \pi_3^{x_3} \ldots \pi_{g_p}^{x_{g_p}} \underset{(l)}{=} \prod_{j=2}^{t} (p_1^{b_j} p_j)^{h_k k^* y_j} \quad \text{in } k$$

where $x_1, \ldots, x_{g_p}$ and $y_2, \ldots, y_t$ are rational integers. If $g_{p_j} = 1$ $(2 \leqslant j \leqslant t)$, then $y_j \equiv 0 \bmod l$ by (1) and (8). For $p = p_1$ we derive from (1) and (8)

$$\sum_{i=2}^{g_p} a_i x_i \equiv \sum_{j=2}^{t} b_j y_j \bmod l,$$

$$x_2 \equiv \ldots \equiv x_{g_p} \equiv \sum_{j=2}^{t} b_j y_j \bmod l.$$

Hence $(\sum_{i=2}^{g_p} a_i - 1)\sum_{j=2}^{t} b_j y_j \equiv 0 \bmod l$. If $\sum_{j=2}^{t} b_j y_j \not\equiv 0 \bmod l$, then $\sum_{i=2}^{g_p} a_i \equiv 1 \bmod l$. Since $\mathfrak{l}$ is unramified in $k(\sqrt[l]{\pi_1^{a_2}\pi_2}), \ldots, k(\sqrt[l]{\pi_1^{a_{g_p}}\pi_{g_p}})$, $\mathfrak{l}$ is unramified in $k(\sqrt[l]{\pi_1^{\sum a_i}\pi_2 \ldots \pi_{g_p}}) = k(\sqrt[l]{p_1})$ which is contrary to the fact $p_1^{l-1} \not\equiv 1 \bmod l^2$. For $p = p_j$ with $g_{p_j} > 1$ $(2 \leqslant j \leqslant t)$ we have

$$\sum_{i=2}^{g_p} a_i x_i \equiv y_j \bmod l,$$

$$x_2 \equiv \ldots \equiv x_{g_p} \equiv y_j \bmod l.$$

Hence $(\sum_{i=2}^{g_p} a_i - 1)y_j \equiv 0 \bmod l$. If $y_j \not\equiv 0 \bmod l$, then $\sum_{i=2}^{g_p} a_i \equiv 1 \bmod l$ and $\mathfrak{l}$ is unramified in $k(\sqrt[l]{p_j})$, a contradiction. We see that $y_2 \equiv \ldots \equiv y_t \equiv 0 \bmod l$ and $\mu \underset{(l)}{=} 1$ in k. Thus $k_1'(l, m_1) \cap k_2'(l, m_1) = k$. It then follows that

$$(k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l) : k) = \prod_{p|m_1} l^{g_p - 1} \cdot l^{t-1} \cdot \prod_{q|m_0} l^{g_p} = \prod_{p|m} l^{g_p}/l.$$

(ii) If $m^{l-1} \equiv 1 \bmod l^2$, then $t \geqslant 2$ and $m_1^{l-1} \equiv 1 \bmod l^2$. Since $(p_1^{b_j} p_j)^{l-1} \equiv 1 \bmod l^2$ for $j = 2, \ldots, t$, we have

$$p_1^{(\Sigma b_j - 1)(l-1)}(p_1 \ldots p_t)^{l-1} \equiv 1 \bmod l^2.$$

Hence

$$p_1^{(\Sigma b_j - 1)(l-1)} \equiv 1 \bmod l^2 \quad \text{where} \quad p_1^{l-1} \not\equiv 1 \bmod l^2.$$

Consequently we have $\sum_{j=2}^{t} b_j \equiv 1 \bmod l$. We then observe that

$$k(\sqrt[l]{m_1}) = k(\sqrt[l]{p_1^{\Sigma b_j} p_2 \ldots p_t})$$

is a subfield of $k_2'(l, m_1)$. For each prime factor q of m_0 it is clear that $k(\sqrt[l]{q})$ is a subfield of $K_0^*(l) = \prod_{q|m_0} k^*(l, q)$, thus $K = k(\sqrt[l]{m})$ is a subfield of $k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l)$.

Combining all these results and (5), (6), (7) we have

THEOREM 3. *Let $l \geqslant 5$ be a regular prime. Let $K^*(l)$ be the l-genus field of $K = k(\sqrt[l]{m})$ or $K = k(\sqrt[l]{lm})$ over k where m is the l-th power free rational integer satisfying* (3) *and* (4).

Then we have

$$K^*(l) = K \cdot k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l),$$

$$(K^*(l) : K) = \begin{cases} \prod_{p|m} l^{g_p}/l^2, & \text{if } m^{l-1} \equiv 1 \bmod l^2 \text{ and } K = k(\sqrt[l]{m}), \\ \prod_{p|m} l^{g_p}/l, & \text{otherwise;} \end{cases}$$

and $(E_k : E_k \cap N_{K/k}K) = l$.

Proof. Let $K = k(\sqrt[l]{m})$ and $m^{l-1} \equiv 1 \bmod l^2$. Then $\mathfrak{l}$ is unramified in K and $t \geqslant 2$. Applying Abhyanker's Lemma and Lemma 7 we see that $K \cdot k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l)$ is an unramified Abelian extension of degree $\prod_{p|m} l^{g_p}/l^2$ over K and also a subfield of $K^*(l)$. By the genus number formula we obtain

$$(K^*(l) : K) = \prod_{p|m} l^{g_p}/l(E_k : E_k \cap N_{K/k}K).$$

Hence $(E_k : E_k \cap N_{K/k}K) \leqslant l$. If $(E_k : E_k \cap N_{K/k}K) = 1$, then ζ is a norm in K/k. It is clear that $\zeta \in N_{K/k}K \Leftrightarrow p^{l-1} \equiv 1 \bmod l^2$ for all prime factors p of m (cf. proof of Proposition 2). Since $t \geqslant 2$, $(E_k : E_k \cap N_{K/k}K) = l$, as desired.

Let $K = k(\sqrt[l]{m})$ and $m^{l-1} \not\equiv 1 \bmod l^2$. Then $\mathfrak{l}$ is ramified in K, but unramified in $k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l)$. Hence $K \cap k_1'(l, m_1) \cdot k_2'(l, m_1) \times \times K_0^*(l) = k$. Applying Abhyanker's Lemma and Lemma 7 we see that $K \cdot k_1'(l, m_1) \cdot k_2'(l, m_1) \cdot K_0^*(l)$ is an unramified Abelian extension of degree $\prod_{p|m} l^{g_p}/l$ over K and a subfield of $K^*(l)$. By the genus number formula of K over k we obtain

$$(K^*(l) : K) = l \prod_{p|m} l^{g_p}/l(E_k : E_k \cap N_{K/k}K) = \prod_{p|m} l^{g_p}/(E_k : E_k \cap N_{K/k}K),$$

where $(E_k : E_k \cap N_{K/k}K) = l$, since $t \geqslant 1$. Thus we have the assertion.

Finally, let $K = k(\sqrt[l]{lm})$. Then $\mathfrak{l}$ is ramified in K. Thus we have the same proof as stated above.

For example, let $l = 7$ and $m = 2 \cdot 3 \cdot 41$. Then $2^3 \equiv 3^6 \equiv 41^2 \equiv 1 \bmod 7$; $2^6 \not\equiv 1$, $3^6 \not\equiv 1$, $41^6 \not\equiv 1 \bmod 7^2$, but $m \equiv 1 \bmod 7^2$. Let $K = k(\sqrt[7]{m})$ where k is the 7-th cyclotomic field. Then $(K^*(7) : K) = 7^{2+1+3}/7^2 = 7^4$.

References

[1] S. I. Borewicz und I. R. Šafarevič, *Zahlentheorie*, Birkhäuser Verlag, 1966.

[2] G. Frey und W. D. Geyer, *Über die Fundamentalgruppe von Körpern mit Divisorentheorie*, J. Reine Angew. Math. 245 (1972), pp. 110–122.

[3] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), pp. 281–285.

[4] F. Gerth III, *On 3-class groups of cyclic cubic extensions of certain number fields*, J. Number Theory 8 (1976), pp. 84–98.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica Verlag, 1965.

[6] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Gesammelte Abhandlungen, Bd. I, Springer Verlag, 1970.

[7] S. Kobayashi, *On the l-dimension of the ideal class groups of Kummer extensions of a certain type*, J. Fac. Sci. Univ. Tokyo 18 (1971), pp. 399–404.

[8] M. L. Madan, *Class groups of global fields*, J. Reine Angew. Math. 252 (1972), pp. 171–177.

[9] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo* p^{N+1}, Nagoya Math. J. 73 (1979), pp. 41–60.
[10] C. J. Parry and C. D. Walter, *The class number of pure fields of prime degree*, Mathematika 23 (1976), pp. 220–226; 24 (1977), p. 133.
[11] R. W. van der Waall, *On the conductor of the non-Abelian simple character of the Galois group of a special field extension*, Symposia Math. 15 (1975), pp. 389–395.
[12] H. Wada, *On cubic Galois extensions of* $Q(\sqrt{-3})$, Proc. Japan Acad. 46 (1970), pp. 397–400.
[13] H. Yokoi, *On the divisibility of the class number in an algebraic number field*, J. Math. Soc. Japan 20 (1968), pp. 411–418.

DEPARTMENT OF MATHEMATICS
TOYAMA UNIVERSITY
Gofuku 3190, Toyama 930, Japan

Received on 17.6.1982
and in revised form on 28.2.1983 (1312)

ACTA ARITHMETICA
XLIV (1984)

Irreducible discriminant components of coefficient spaces

by

M. Fried (Irvine, Cal.)* and J. Smith (Boston, Mass.)

1. Introduction and notation. Let A^n_R and A^n_C be two copies of affine n-space defined over Q. The *Noether cover* is the Galois cover (with group S_n) associated to the map $A^n_R \xrightarrow{\Phi_n} A^n_C$ that sends $(y(1), \ldots, y(n))$ to the n-tuple of symmetric functions

$$(x(1), \ldots, x(n)) = \Big(\ldots, (-1)^i \sum_{j(1)<\ldots<j(i)} y(j(1))\cdot \ldots \cdot y(j(i)), \ldots\Big).$$

For $\{i(1), \ldots, i(u)\} = I$ a subset of $\{1, 2, \ldots, n\}$, the *coefficient locus* $X(I)$ is defined by the equations $x(i) = 0$ for all $i \notin I$.

The *discriminant locus* is the image in A^n_C of the points of A^n_R for which two or more entries are equal. We identify the irreducible components of the intersection of $X(I)$ with the discriminant locus. If the elements of I have no common divisor, besides some trivial components (hyperplanes), this intersection is irreducible (Theorem 3.1).

Cohen [1] has shown that the Galois group of the cover induced by certain subvarieties of $X(I)$ is S_n. An easy consequence of the above irreducibility is a less sharp result: the group of the cover induced over $X(I)$ is S_n. Examples show (§ 4) that our results may remain valid for all of Cohen's subvarieties.

For F a field, $\bar{F}$ is a fixed algebraic closure of F. Let $A^n_R(\bar{F})$ denote the n-tuples of elements $(y(1), \ldots, y(n)) \in (\bar{F})^n$. The subscript R (for "roots") indicates that the n-tuple is regarded as an ordering on the roots of the monic polynomial

$$\prod_{i=1}^{n} (y - y(i)) = p(y) = y^n + \sum_{i=1}^{n} x(i)\cdot y^{n-i}.$$

Let $A^n_C(\bar{F})$ denote another copy of affine n-space: the subscript C (for "coefficients") indicates that the points of $A^n_C(\bar{F})$ correspond to the coefficients of monic polynomials of degree n.

For X defined by equations with coefficients in F ([3], p. 181), X is F-

* Supported by N.S.F. Grant MCS 80-03253.